RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0A1 / Noyau 0A1
Gatineau, Québec K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires
THIS REQUIREMENT CONTAINS A SECURITY REQUIREMENT - SEE PART 6.

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Business Management and Consulting Services Division / Division des services de gestion des affaires et de consultation
11 Laurier St. / 11, rue Laurier
10C1, Place du Portage
Gatineau, Québec K1A 0S5

Title - Sujet PCI CONSULTANT	
Solicitation No. - N° de l'invitation EN891-121307/B	**Amendment No. - N° modif.** 003
Client Reference No. - N° de référence du client 20121307	**Date** 2012-05-15
GETS Reference No. - N° de référence de SEAG PW-$$ZG-406-24295	
File No. - N° de dossier 406zg.EN891-121307	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2012-05-29**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Harrington, Ingrid	**Buyer Id - Id de l'acheteur** 406zg
Telephone No. - N° de téléphone (819) 956-3201 ( )	**FAX No. - N° de FAX** (819) 956-2675
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

La présente demande de modification 001 vise à répondre aux questions relatives à la demande de propositions (DP) tel que détaillé ci-dessous.

Questions et réponses

Nous voulons poser les questions suivantes en ce qui concerne la demande de propositions (DP) susmentionnée**.**

Q11. Question 1 (Référence : Pièce jointe 1 de la partie 4 [Critères techniques])

Conformément au critère technique obligatoire CTO1, le soumissionnaire doit avoir détenu la certification d'évaluateur de sécurité qualifié (QSA) pendant au moins quatre (4) ans. Notre entreprise détient une certification QSA délivrée par le PCI Security Standards Council depuis octobre 2008. De plus, nous fournissons des conseils et des services d'assurance en matière de sécurité de l'information à des organisations des secteurs privé et public, y compris à des institutions financières, aux fournisseurs de services de télécommunication et aux fournisseurs de services Internet, depuis de nombreuses années, ce qui satisfait à l'essence même de cette exigence. Nous pouvons résumer cela dans la proposition. Notre équipe détient également une solide expertise en ce qui a trait à la conformité aux normes PCI DSS qui, à notre avis, satisferait à l'essence même de cette exigence. L'État pourrait-il envisager de modifier le critère CTO1 pour accepter les soumissionnaires qui détiennent une certification QSA et qui possèdent au moins quatre ans d'expérience pertinente par rapport à l'énoncé des travaux de la DP dans la fourniture de conseils et de services d'assurance en matière de sécurité de l'information comme équivalent à la certification QSA de quatre ans exigée dans les secteurs des services financiers et des paiements ainsi que dans le secteur public?

R11. Veuillez consulter la réponse fournie à la question 3 dans la modification 001 à la demande de soumissions.

Q12. Question 2 (Référence : Pièce jointe 1 de la partie 4 [Critères techniques])

Conformément au critère technique obligatoire CTO1, le soumissionnaire doit avoir détenu la certification de prestataire de services d'analyse agréé (ASV) pendant au moins quatre (4) ans. Notre entreprise détient une certification de prestataire de services d'analyse agréé depuis deux ans (du milieu de 2009 au milieu de 2011) accordée par le PCI Security Standards Council depuis octobre 2008. Nous effectuons des analyses des vulnérabilités et des tests de pénétration de réseaux et de systèmes pour des organisations des secteurs privé et public, y compris pour des institutions financières, depuis de nombreuses années, ce qui satisfait à l'essence même de cette exigence. Nous pouvons résumer cela dans la proposition. L'État pourrait-il envisager de modifier le critère CTO1 pour accepter les soumissionnaires qui détiennent au moins quatre ans d'expérience pertinente par rapport à l'énoncé des travaux de la DP dans la conduite d'analyses des vulnérabilités et de tests de pénétration de réseaux et de systèmes comme équivalent à la certification ASV de quatre ans exigée?

R12. Veuillez consulter la réponse fournie à la question 3 dans la modification 001 à la demande de soumissions.

Q13. Question 3 (Référence : section 2 de la partie 1)

La DP indique que les ressources devront " effectuer un examen approfondi du déroulement des activités ministérielles et des contrôles de sécurité ". La section 3.1 de l'annexe A - Énoncé des travaux - Conseiller en conformité à la norme PCI DSS, indique que l'entrepreneur doit effectuer un " examen de la transmission des données de titulaires de carte de chacun des ministères ". Est-ce que l'exigence figurant

à la section 2 de la partie 1 est la même que l'exigence figurant à l'annexe A? Le Canada exige-t-il un examen du déroulement des opérations qui ne constituent pas une transmission des données de titulaires de carte? Dans l'affirmative, dans quel but (si ce n'est pas pour assurer la conformité aux normes PCI DSS)?

R13. Le Canada souhaite examiner la transmission des données de titulaires de carte pour assurer la conformité aux normes PCI DSS. La section 2 de la partie 1 ainsi que la section 3.1 de l'annexe A de la DP font référence aux secteurs d'activité où les cartes de crédit sont généralement acceptées et la transmission des données de titulaires de carte est assurée.

Q14. Question 4 (Référence : section 2 de la partie 1)

Est-ce que les ministères visés par la portée auront des documents complets sur le déroulement des activités pertinentes, la transmission des données de titulaires de carte et les contrôles de sécurité aux fins d'examen par l'expert-conseil? Avant l'examen, l'expert-conseil devra-t-il fournir des directives aux ministères en ce qui a trait à la préparation de ces documents?

R14. Pour ce qui est des données de titulaires de cartes et des contrôles de sécurité, il se peut que les ministères n'aient aucun document détaillé sur le déroulement des activités. Par conséquent, l'expert-conseil devra peut-être fournir des directives aux ministères relativement à la préparation des documents.

Q15. Question 5 (Référence : section 2 de la partie 1)

Lieu de travail - Est-ce que l'État peut fournir, de façon approximative, une répartition des travaux qui seront exécutés dans nos locaux (dont certains pourraient être situés à l'extérieur de la région de la capitale nationale [RCN]) et des travaux/réunions qui auront lieu dans la RCN?

R15. La majeure partie des travaux peut se faire dans les locaux du soumissionnaire. Toutefois, une réunion de lancement aura lieu dans les bureaux du Receveur général de la RCN; plusieurs administrations centrales ministérielles se situent également dans la RCN. Les soumissionnaires devraient tenir compte de ces facteurs au moment de proposer des plans de travail.

Q16. Question 6 : section 4 de la partie 1

Question 6 : section 4 de la partie 1 - Interdiction de soumissionner les besoins connexes futurs. Nous comprenons et appuyons cette interdiction. Après la période d'exécution, combien de temps le Canada s'attend-il à ce que cette interdiction soit en vigueur?

R16. L'interdiction est associée aux exigences figurant à l'article 3.3 - Autres exigences en matière d'approvisionnement du QSA et du ASV, de l'annexe A - Énoncé des travaux.

Q17. Question 7 (Référence : section 3 - Exigences relatives à la sécurité, de la partie 7)

Conformément à la section 3 - Exigences relatives à la sécurité, de la partie 7, les membres du personnel de l'entrepreneur doivent détenir une cote de sécurité du personnel valable au niveau SECRET. Dans le cadre de la présente DP, nous prévoyons proposer a) des partenaires d'une grande firme de comptables agréés/d'experts-conseils dont l'un a déjà détenu une cote de sécurité secrète et b) une autre personne qui a occupé des postes de direction dans des institutions financières et des entreprises fournissant des services de technologie de l'information. Pouvons-nous commencer à fournir les services requis dans le cadre de la présente DP si nos employés détiennent uniquement une cote de fiabilité approfondie, mais qu'ils ont rempli et soumis les demandes d'autorisation de sécurité de niveau Secret? Il est toutefois

entendu qu'ils ne pourront accéder aux documents et aux renseignements classifiés tant qu'ils n'auront pas obtenus les cotes de sécurité de niveau Secret.

R17. Veuillez consulter la réponse fournie à la question 2 dans la modification 001 à la demande de soumissions. De plus, avant l'attribution du contrat, le conseiller principal en conformité à la norme PCI DSS et le conseiller en conformité à la norme PCI DSS proposé par le soumissionnaire doit satisfaire aux exigences de sécurité indiquées à la partie 7 - Clauses subséquentes du contrat.

Q18. Question 8 (Référence : section 3.0 - Portée des travaux, de l'annexe A - Énoncé des travaux - Conseiller en conformité à la norme PCI DSS)

Les services consultatifs relatifs à la norme PCI DSS décrits à la section 3.0 - Portée des travaux, de l'annexe A - Énoncé des travaux - Conseiller en conformité à la norme PCI DSS, comprennent certaines activités que l'État aurait peut-être avantage, sur les plans de l'efficacité, de l'efficience et de la rentabilité, à confier à des membres du personnel qui possèdent moins d'expérience et, par conséquent, coûtent moins cher que le conseiller principal en conformité à la norme PCI DSS et le conseiller en conformité à la norme PCI DSS. Voici des exemples :

- 3.1 Atteinte de la conformité à la norme PCI DSS :
  - o déterminer les mesures de sécurité et les contrôles internes relatifs aux rapports financiers dans chaque ministère;
  - o adapter les évaluations de la norme PCI DSS disponibles sur le site du PCS Security Standards Council aux processus opérationnels de chacun des ministères, y compris la bonne application des contrôles compensatoires;
  - o fournir des évaluations de l'état de préparation à la vérification de la conformité à la norme PCI DSS en vue de déterminer […] le degré actuel de conformité pour les projets et les environnements compris dans la portée […];
  - o élaborer un programme de vérification et le communiquer aux ministères.

- 3.2 Transfert des connaissances
  - o la formation du RG et des ministères sur l'utilisation des contrôles compensatoires.

Est-ce que l'État envisagerait de nous permettre de fournir des personnes autres que des cadres et des personnes expérimentées pour assumer les rôles de " conseiller principal en conformité à la norme PCI DSS " et de " conseiller en conformité à la norme PCI DSS ", comme il est indiqué dans la DP, afin que nous puissions proposer des membres subalternes de l'équipe pour exécuter certains travaux sous la supervision directe du " conseiller principal en conformité à la norme PCI DSS " et du " conseiller en conformité à la norme PCI DSS ", selon le cas, après qu'une autorisation de tâche ait été convenue avec le chargé de projet, conformément à la partie 7 de la DP. Si c'est acceptable, pouvons-nous attribuer une partie des tâches à un conseiller subalterne en conformité à la norme PCI DSS (pièce jointe 1 de la partie 3 - Barème de prix)?

R18. Veuillez consulter la réponse fournie à la question 8 dans la modification 002 à la demande de soumissions.

Q19. Question 9 (Référence : section 7.4 - Langue de travail, de l'annexe A - Énoncé des travaux - Conseiller en conformité à la norme PCI DSS)

Les personnes que nous avons indiquées qui pourraient le mieux fournir au Canada les services consultatifs relatifs à la norme PCI DSS décrits à la section 3.0 de l'annexe A ne sont pas bilingues (ils ne parlent pas français). L'État envisagerait-il de nous permettre d'ajouter une ressource bilingue subalterne à notre équipe qui pourrait aider le conseiller principal et le conseiller en conformité à la norme PCI DSS à

fournir des services en français si nécessaire? Cette ressource subalterne ferait aussi partie de l'équipe qui réaliserait les activités mentionnées à la section 3.0 de l'annexe A, si celles-ci peuvent être réalisées de façon satisfaisante par des employés moins expérimentés.

R19. Le Canada a révisé l'article 7.4 - Langue de travail, de l'annexe A - Énoncé des travaux. Veuillez consulter la réponse fournie à la question 5.2 dans la modification 001 à la demande de soumissions. Le Canada a également révisé l'exigence de façon à y inclure un conseiller subalterne en conformité à la norme PCI DSS; veuillez consulter la réponse fournie à la question 8 dans la modification 002 à la demande de soumissions

Q20. Question 10 : (Référence : partie 1 - Clôture de l'invitation)

Afin de nous assurer que nous abordons toutes les exigences révisées de la DP découlant des réponses fournies aux questions soumises, l'État envisagerait-il de reporter la date de présentation de la DP au 29 mai 2012?

R20. Le Canada a reporté la date de clôture de la soumission du 15 mai 2012 au 29 mai 2012. Veuillez consulter l'article 2 de la modification 002 à la demande de soumissions.

Q21. Question 11 (Référence : pièce jointe 1 de la partie 4)

En ce qui a trait à la définition d'un soumissionnaire, un de nos principaux membres de l'équipe est un sous-traitant de notre entreprise. Pouvez-vous préciser si cela est acceptable étant donné que le sous-traitant sait qu'il sera inclus dans l'équipe proposée en réponse à cette DP et en convient?

R21. Veuillez consulter la réponse fournie à la question 1 dans la modification 001 à la demande de soumissions. Il est possible de proposer un sous-traitant en réponse aux CTO3 et CTO4 de la pièce jointe 1 à partie 4 - Critères techniques obligatoires, et au CTC1.1 des Critères techniques cotés.